JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11)Publication number: 07249264
(43)Date of publication of application: 26.09.1995

(51)Int.Cl.
G11B 20/10
G06F 12/14

(21)Application number: 06065426
(22)Date of filing: 10.03.1994

(71)Applicant: INTEC:KK
BROTHER IND LTD
(72)Inventor: KAWASAKI TETSUO
HOSHIBA SHINJI
TANIGUCHI TOSHINORI

(54) RECORDING SYSTEM AND RECORDING/REPRODUCING SYSTEM FOR CD-ROM, AND CD-ROM DISK

(57)Abstract:

PURPOSE: To unnecessitate control of key information for deciphering ciphered data recorded in a CD-ROM disk.
CONSTITUTION: When desired information is ciphered and recorded in the CD- ROM disk 1, key information required for decoding this ciphered information is recorded in a proper region 3 in the CD-ROM disk 1 with the ciphering information. When recorded contents of the CD-ROM disk 1 in which ciphering information is recorded by this recording system are reproduced, a desired key information is read out from the same CD-ROM disk 1 with ciphering information, and the ciphered information can be deciphered by only this read- out information.

(19)日本国特許庁(JP)　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平７－２４９２６４

(43)公開日　平成7年(1995)9月26日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｇ１１Ｂ　20/10		Ｈ　7736－５Ｄ		
Ｇ０６Ｆ　12/14	３２０　Ｂ			

審査請求　未請求　請求項の数３　ＦＤ　（全９頁）

(21)出願番号　特願平6-65426

(22)出願日　平成6年(1994)3月10日

(71)出願人　391021710
株式会社インテック
富山県富山市牛島新町5番5号

(71)出願人　000005267
ブラザー工業株式会社
愛知県名古屋市瑞穂区苗代町15番1号

(72)発明者　河崎　哲男
富山県富山市下新町3番23号　株式会社インテック内

(72)発明者　千場　進二
富山県富山市下新町3番23号　株式会社インテック内

(74)代理人　弁理士　高野　昌俊

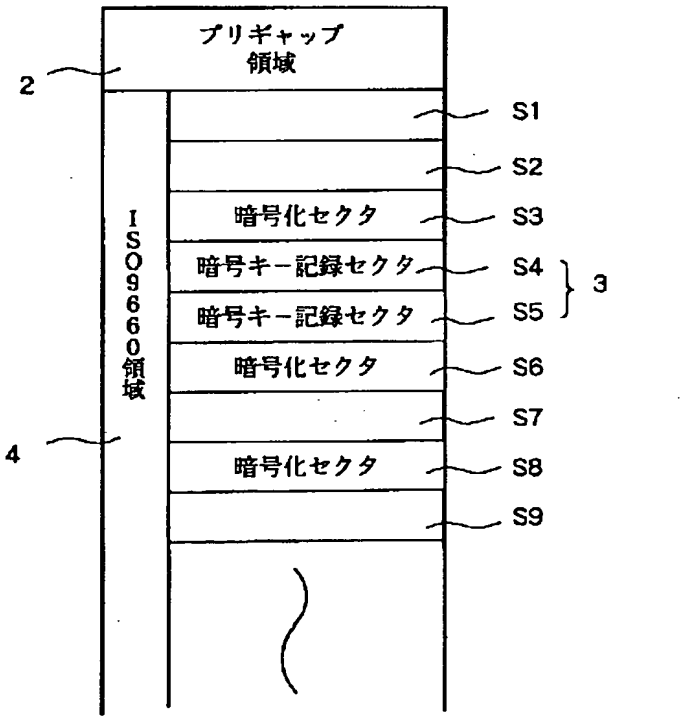
最終頁に続く

(54)【発明の名称】ＣＤ－ＲＯＭの記録方式、記録・再生方式及びＣＤ－ＲＯＭディスク

(57)【要約】

【目的】　ＣＤ－ＲＯＭディスクに記録された暗号化データの解読のためのキー情報の管理を不要にすること。

【構成】　所要の情報を暗号化してＣＤ－ＲＯＭディスク（１）に記録するさい、この暗号化情報を復号化するのに必要なキー情報を該暗号化情報と共に該ＣＤ－ＲＯＭディスク（１）内の適宜の領域（３）に記録する。このような記録方式で暗号化情報が記録されているＣＤ－ＲＯＭディスクの記録内容を再生する場合には、暗号化情報と共に所要のキー情報が同一のＣＤ－ＲＯＭディスクから読み出され、これらの読み出し情報のみによって暗号化情報を復号化することができる。



1

【特許請求の範囲】

【請求項１】　所要の情報を暗号化してＣＤ－ＲＯＭディスクに記録するためのＣＤ－ＲＯＭの記録方式において、ＣＤ－ＲＯＭディスクに記録すべき暗号化情報を復号化するのに必要なキー情報を該暗号化情報と共に該ＣＤ－ＲＯＭディスク内に記録しておくことを特徴とするＣＤ－ＲＯＭの記録方式。

【請求項２】　所要の情報を暗号化してＣＤ－ＲＯＭディスクに記録しこの記録された暗号化情報をＣＤ－ＲＯＭディスクから読み出して復号化するためのＣＤ－ＲＯＭの記録・再生方式において、ＣＤ－ＲＯＭディスクに記録すべき暗号化情報を復号化するのに必要なキー情報を該暗号化情報と共に該ＣＤ－ＲＯＭディスク内に記録しておき、再生時にはＣＤ－ＲＯＭディスク内に記録されている暗号化情報とキー情報とを読み出し、ＣＤ－ＲＯＭディスクから読み出されたキー情報を使用して該暗号化情報を復号化することを特徴とするＣＤ－ＲＯＭの記録・再生方式。

【請求項３】　所要の情報が暗号化されて記録されているＣＤ－ＲＯＭディスクにおいて、記録された暗号化情報を復号するのに必要なキー情報が該ＣＤ－ＲＯＭディスク内に記録されていることを特徴とするＣＤ－ＲＯＭディスク。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、暗号化された各種情報をＣＤ－ＲＯＭディスクに記録し、再生するための、ＣＤ－ＲＯＭの記録方式、ＣＤ－ＲＯＭの記録・再生方式、及びＣＤ－ＲＯＭディスクに関するものである。

【０００２】

【従来の技術】大量の情報を記録するため、レーザ光等を用いた光学式の記録・再生方式が公知であり、このための光ディスクとして、特にコンパクトディスク読出し専用メモリ、所謂ＣＤ－ＲＯＭディスクがオーディオの分野のみならず各種の分野で広く用いられている。ＣＤ－ＲＯＭディスクは一般に再生専用型の記録媒体として用いられてきたが、近年追記型のものも開発され、実用に共されている。

【０００３】ところで、再生専用型であれ追記型であれ、ＣＤ－ＲＯＭディスクに書き込まれる情報の機密保持のため、記録すべき情報を暗号化し、この暗号化された情報をＣＤ－ＲＯＭディスクに記録するという要求がしばしば生じる。このような要求を満たす１つの技術として、例えば、特開昭６４－９１２５６号公報の第４頁上左欄において説明されているように、ＣＤ－ＲＯＭディスクにユーザデータを記録させる際に暗号データを付加したスクランブル処理を施して暗号化データにして記録させ、ＣＤ－ＲＯＭドライバにより暗号化データをデ・スクランブル処理を施した後、インターフェースにより復号データ（暗号データと同一）と暗号化データとを

2

排他論理処理を施してからコンピュータに出力し、これによりユーザデータのセキュリティを確実に行うことができるようにした技術が公知である。この従来技術は、所要の情報をハードウェアを用いて復号化処理する構成であるから、ソフトウェアにより処理を利用する場合に比べ処理の時間を大幅に短縮することができる点に大きな特徴を有している。

【０００４】

【発明が解決しようとする課題】しかしながら、上述した従来技術によると、復号化のためのキーとハードウェアとが密接に関連しているため、もしキーの変更が必要な場合にはハードウェアの変更若しくは復号ＲＡＭ内容の変更をしなければならず、キーの変更のために相当のコストが必要となる。したがって、固定キーを使用し続ける傾向を生じ、第三者がＣＤ－ＲＯＭディスクの記録内容を解読するための手掛りを得ることを比較的容易ならしめる結果になるという問題点を有している。これは、ＣＤ－ＲＯＭディスクに記録すべきデータのフォーマットがＩＳＯ９６６０で規格化されているため、同一のキーを継続して使用すると、規格で定められた特定の内容が格納されているアドレスのデータ内容を手掛りに復号化のためのキーを比較的容易に推測することができるとの理由による。そして、このようにして復号化のためのキーが第三者に一旦知れてしまうと、残りのＣＤ－ＲＯＭディスクの記録内容も直ちに解読されてしまうという不具合を生じる。

【０００５】上記従来技術による他の問題点は、復号化のためのキーの内容は、予め適宜の手段、例えばコードブックに記載しておく等の手段により管理しておかねばならないため、キーの管理が別途必要となり、キー情報管理のためのコストが発生することである。この問題点は上記従来技術のみならず、ＣＤ－ＲＯＭディスクに暗号化データを記録しようとする場合、一般に生じる問題点である。

【０００６】本発明の目的は、したがって、従来技術における上述の問題点、不具合等のうちの１つ又はいくつか、或いは全部を改善することができる、ＣＤ－ＲＯＭの記録方式、ＣＤ－ＲＯＭの記録・再生方式、及びＣＤ－ＲＯＭディスクを提供することにある。

【０００７】本発明の目的をより具体的に例示的に列挙すれば次の通りである。

【０００８】ＣＤ－ＲＯＭディスクに記録すべき情報の暗号化のためのキーの変更に伴うキー情報の管理を不要にした、ＣＤ－ＲＯＭの記録方式及びＣＤ－ＲＯＭの記録・再生方式を提供すること。

【０００９】記録された暗号化データの解読のためのキー情報の管理を不要にしたＣＤ－ＲＯＭディスクを提供すること。

【００１０】暗号化して記録されたデータ内容の解読のためのキーを第三者が容易に知ることができないよう、

コストを上昇させることなしに複数の異なったキーを使用できるようにした、ＣＤ－ＲＯＭの記録方式及びＣＤ－ＲＯＭの記録・再生方式を提供すること。

【００１１】ＣＤ－ＲＯＭディスクに記録すべき情報の暗号化及び暗号化された情報を復号化するために必要なキーを記録媒体毎に容易に変更することでができ、且つキーの管理を不要にすることができるようにした、ＣＤ－ＲＯＭの記録方式、ＣＤ－ＲＯＭの記録・再生方式及びＣＤ－ＲＯＭディスクを提供すること。

【００１２】

【課題を解決するための手段】上記課題を解決するため、本発明は、所要の情報を暗号化して光ディスクであるＣＤ－ＲＯＭディスクに記録するためのＣＤ－ＲＯＭの記録方式において、ＣＤ－ＲＯＭディスクに記録すべき暗号化情報を復号化するのに必要なキー情報を該暗号化情報と共に該ＣＤ－ＲＯＭディスク内に記録しておくことを特徴としている。

【００１３】また、本発明は、所要の情報を暗号化してＣＤ－ＲＯＭディスクに記録しこの記録された暗号化情報をＣＤ－ＲＯＭディスクから読み出して復号化するためのＣＤ－ＲＯＭの記録・再生方式において、ＣＤ－ＲＯＭディスクに記録すべき暗号化情報を復号化するのに必要なキー情報を該暗号化情報と共に該ＣＤ－ＲＯＭディスク内に記録しておき、再生時にはＣＤ－ＲＯＭディスク内に記録されている暗号化情報とキー情報とを読み出し、ＣＤ－ＲＯＭディスクから読み出されたキー情報を使用して該暗号化情報を復号化することを特徴としている。

【００１４】さらに、本発明は、所要の情報が暗号化されて記録されているＣＤ－ＲＯＭディスクにおいて、記録された暗号化情報を復号するのに必要なキー情報が該ＣＤ－ＲＯＭディスク内に記録されていることを特徴としている。

【００１５】

【作用】所要の情報を暗号化してＣＤ－ＲＯＭディスク内に記録する際に、その後このＣＤ－ＲＯＭディスクから読み出された暗号化情報を復号化するために必要なキー情報もそのＣＤ－ＲＯＭディスク内に記録される。これにより、暗号化情報とこの解読に必要なキー情報とを常に一体に管理することができる。

【００１６】このような記録方式で暗号化情報が記録されているＣＤ－ＲＯＭディスクの記録内容を再生する場合には、暗号化情報と共に所要のキー情報が同一のＣＤ－ＲＯＭディスクから読み出され、これらの読み出し情報のみによって暗号化情報を復号化することができ、復号化のためのキー情報を特に意識することなしに所要の復号化が実行される。

【００１７】このように、キー情報を適宜に変更しても、ＣＤ－ＲＯＭディスク内には、記録されている暗号化情報の復号化、すなわち解読に必要なキー情報が必ず記録されており、キー情報のみの管理は不要である。

【００１８】

【実施例】以下、図面を参照して本発明の一実施例につき詳細に説明する。

【００１９】図１及び図２には、本発明によりＣＤ－ＲＯＭディスクに所要の情報を記録するためのＣＤ－ＲＯＭ記録システム、及びこれと対をなしてＣＤ－ＲＯＭ記録・再生システムを構成するＣＤ－ＲＯＭ再生システムがそれぞれ示されている。

【００２０】先ず、図１を参照してＣＤ－ＲＯＭ記録システム１０について説明すると、１１はＣＤ－ＲＯＭディスク１に記録すべきユーザデータが予め格納されている記憶装置、１２は各種指令データを入力するためのキーボード、１３はキーボード１２により指示された所要のユーザデータを記憶装置１１から後述するようにして順次読み出すための読出制御部であり、読出制御部１３によって読み出された所要のユーザデータは暗号化ユニット１４に送られる。

【００２１】暗号化ユニット１４についての説明に先立って、ＣＤ－ＲＯＭディスク１に所望のユーザデータを記録するための記録方式について図３を参照して説明する。

【００２２】図３に示されるように、ＣＤ－ＲＯＭディスク１の記録領域は、プリギャップ領域２とＩＳＯ９６６０領域４とに大別され、ＩＳＯ９６６０領域には多数のセクタＳ１、Ｓ２、Ｓ３・・・が設定されている。そして、これらのセクタＳ１、Ｓ２、Ｓ３・・・は、１９８８年に発行されたＩＳＯ９６６０情報交換用ＣＤ－ＲＯＭのボリューウム及びファイルの構造に関するＪＩＳＸ０６０６－１９９０に基づくデータフォーマットに従って構成されている。

【００２３】したがって、記録すべきデータは、各セクタに設けられている２０４８バイトのユーザデータ領域に分割して順次格納され、ＣＤ－ＲＯＭディスク１に記録すべき１セクタ分のデータの内容及びその作成方法についてはその規格に詳述されているので、ここではその詳細を説明するのは省略し、単に、所要のユーザデータは２０４８バイト分づつＩＳＯ９６６０領域４のセクタに分割されて記録されるという点のみを説明するに止める。また、ＩＳＯ９６６０領域４では、データフォーマットの定義により未使用領域を定めることができ、本実施例の暗号キー記録セクタ３として使用する。

【００２４】図１に戻ると、キーボード１２は、さらに、所要のユーザデータをＣＤ－ＲＯＭディスク１へ記録するためにそのユーザデータをセクタに分割記録する場合、どのセクタに記録されるユーザデータを暗号化すべきかを示す暗号化セクタ情報を入力する機能を有している。この暗号化セクタ情報はキーボード１２から暗号化ユニット１４内の暗号キー生成部１５へ送られる。

【００２５】暗号キー生成部１５は、キーボード１２か

ら送られてきた暗号化セクタ情報に基づき、ユーザデータを暗号化して記録すべきセクタに対する固有の暗号キーを所要のセクタ毎に生成し、暗号キー情報とその暗号キーが使用されるセクタの番号情報とが組になった複数組の暗号キーデータを作成、保持しておく機能を有している。

【００２６】これらの暗号キーデータは、暗号キー記録セクタ３を記録するタイミングでＣＤ－ＲＯＭマスタリング装置１８に送り、ＣＤ－ＲＯＭマスタリング装置１８によってこれらの暗号キーデータがＣＤ－ＲＯＭディスク１内の暗号キー記録セクタ３に記録される（図３参照）。

【００２７】一方、読出制御部１３は、記憶装置１１内に格納されている所要のユーザデータを１セクタ分づつ読み出して暗号化ユニット１４の暗号化部１６に送る。暗号化部１６は、市販の暗号化ＩＣを用いて構成することができ、読出制御部１３から１セクタ分のユーザデータを受け取ると、暗号キー生成部１５に対し、このセクタに対する暗号キーを暗号化部１６へ送るよう要求する暗号キー要求信号を出力する。暗号キー生成部１５はこの暗号キー要求信号に応答し、そのセクタに対して暗号キーが用意されている場合には、すなわちそのセクタへ記録すべきユーザデータが暗号化されるべきであるとキーボード１２から指令されている場合には、そのセクタのために予め用意されている暗号キーを暗号化部１６に送る。若しそのセクタが暗号化を指令されていないものであり、したがって暗号キーが用意されていない場合には、暗号キー生成部１５から暗号化部１６へのデータの送信は行わない。

【００２８】したがって、暗号化部１６では、読出制御部１３から１セクタ分づつ送られてくるユーザデータに対し、暗号化が指令されているセクタのものについてだけ暗号キー生成部１５から供給される暗号キーを用いて暗号化し、暗号化された１セクタ分のユーザデータをインターフェイス部１７に送る。一方、暗号化が指令されていないセクタへ記録すべきユーザデータは暗号化されることなく、そのままインターフェイス制御部１７に送られる。

【００２９】インターフェイス制御部１７では、このようにして暗号化された又は暗号化されていないセクタ毎のユーザデータをＣＤ－ＲＯＭマスタリング装置１８に順次送り、これらのセクタ毎のユーザデータはＣＤ－ＲＯＭディスク１のＩＳＯ９６６０領域４に設けられたセクタＳ１、Ｓ２、・・・に所定の手順によって順次記録される。本実施例では、図３から判るように、セクタＳ１、Ｓ２、Ｓ７、Ｓ９・・・に記録されているユーザデータは暗号化されておらず、セクタＳ３、Ｓ６、Ｓ８・・・に記録されているユーザデータは暗号化されている。また、セクタＳ４、Ｓ５は未使用領域として定義し、暗号キーを記録するセクタとして使用される。しかし、どのセクタのユーザデータを暗号化するか及びどの未使用領域に暗号キーを記録するかは、この一実施例のものに限定されず、適宜に設定することができる。また、キーボード１２からその都度指令するのに代えて、暗号化して記録すべきセクタは第１番目から第２００番目までなどのように固定化しておいてもよい。

【００３０】いずれにせよ、ユーザデータがＣＤ－ＲＯＭディスク１内の所定の領域に暗号化されて、又は暗号化されることなしにセクタ情報として記録され、一方、このようにして記録されたユーザデータを復号化するのに必要な暗号キーがそれと同一のＣＤ－ＲＯＭディスク１内の所定の領域に記録されている点に大きな特徴を有している。この特徴による利点の１つは、暗号キーの管理が不要になることであり、特にＣＤ－ＲＯＭディスク１に記録された暗号化データを再生して復号化する場合に、外部から別途暗号キー情報を与える必要がないことである。

【００３１】なお、上記実施例では、暗号キーをセクタ毎に別のものとしたが、全ての暗号化セクタの暗号キーを同一にしてもよいことは勿論である。暗号キーを多数用いても暗号キー管理の煩らわしさは生じないので、セクタ毎に暗号キーを変えれば、暗号キー管理のコストを上昇させることなしに第三者によるユーザデータの解読を困難にし、機密保持能力を格段に向上させることができる。

【００３２】次に、図２を参照して、図１のＣＤ－ＲＯＭ記録システム１０によりＣＤ－ＲＯＭディスク１に暗号化して記録されたユーザデータを再生、復号化するためのＣＤ－ＲＯＭ再生システム２０について説明する。

【００３３】ＣＤ－ＲＯＭ再生システム２０は、ＣＤ－ＲＯＭディスク１の記録内容を読み取るためのＣＤ－ＲＯＭドライブ装置２１を有している。ＣＤ－ＲＯＭディスク１をＣＤ－ＲＯＭドライブ装置２１にセットすることにより、ＣＤ－ＲＯＭディスク１の暗号キー記録セクタ３に記録されている暗号キーデータが先ず読み出され、インターフェイス制御部２２に送られる。そして、読み出された暗号キーデータは復号化ユニット２３内のメモリ２５内に格納される。

【００３４】しかる後、インターフェイス制御部２２の制御の下に、ＣＤ－ＲＯＭディスク１内のＩＳＯ９６６０領域４に記録されている最初の１セクタ（Ｓ１）がＣＤ－ＲＯＭドライブ装置２１によって読み出され、インターフェイス制御部２２を介して復号化部２４に送られる。復号化部２４もまた、市販の復号化ＩＣを使用して構成することができる。復号化部２４では、このセクタＳ１に対応する暗号キーの読み出しをメモリ２５に対して要求する。

【００３５】本実施例では、セクタＳ１は暗号化セクタではないため、メモリ２５内にはセクタＳ１に対応する暗号キーは格納されていない。したがって、メモリ２５

からは何等の暗号キー情報は出力されず、セクタＳ１内に記録されているユーザデータはそのまま復号化部２４から出力され、バッファメモリ２６内に格納される。セクタＳ２に記録されているユーザデータも全く同様にして処理される。

【００３６】セクタＳ３の記録内容が復号化部２４に入力されると、セクタＳ３に記録されている暗号化ユーザデータを復号化するのに必要な暗号キーが暗号キーデータ中の番号情報を手掛りとして選択され、所要の暗号キーがメモリ２５から復号化部２４に送られる。復号化部２４では、この暗号キーを用いてセクタＳ３に記録されていた暗号化ユーザデータの復号化処理が実行され、復号化されたユーザデータがバッファメモリ２６に送られる。

【００３７】このようにして、セクタＳ１、Ｓ２・・・に記録されていたユーザデータのうち暗号化されていたものは、メモリ２５から供給される暗号キーによ復号されてバッファメモリ２６に送られることになる。一方、暗号化されていなかったユーザデータは復号化ユニット２３をそのまま通過し、バッファメモリ２６に格納される。したがって、バッファメモリ２６から、暗号化をする前の所要のユーザデータ、すなわち復号化されたユーザデータを取り出すことができる。また、セクタＳ４、Ｓ５には暗号キーが記録されているが、データフォーマット上未使用領域であり、ユーザデータの取り出しには影響しない。

【００３８】図１、図２に示したシステムを用いることにより、少なくとも次の如き効果が期待される。

【００３９】ユーザデータを暗号化するのに使用された暗号キーが暗号化されたユーザデータを記録するＣＤ－ＲＯＭディスク１内に一緒に記録されるので、暗号化のキー情報を別途管理する必要がない。したがって、暗号キーの管理のためのコストが不要であるばかりか、その管理の煩わしさから解放される。

【００４０】さらに、暗号化ユーザデータと暗号キーとを同一ＣＤ－ＲＯＭディスク１内に記録するので、暗号キーをどのように変更したとしてもこの変更を別途に記録しておく必要はなく、再生時には復号化に必要な暗号キーをそのＣＤ－ＲＯＭディスク１から読み出すだけでよいから、復号化に要する手間が著しく簡素化される。

【００４１】この方式によりユーザデータの暗号化記録が行われたＣＤ－ＲＯＭディスク１は、暗号キー情報が記録されているので、ＣＤ－ＲＯＭディスク１に対応する暗号キー情報の管理という概念はなく、暗号キー情報管理は全く不要になり、暗号化を全く意識することなしにユーザデータの再生、復号化を行うことができる。

【００４２】このように、暗号キー情報の管理コストが全く問題とならないので、例えばＣＤ－ＲＯＭディスク１毎に異なった暗号キーを使用しても何等のコストを発生させることがなく、記録の機密保持をコストを生じさせることなしに著しく向上させることができる。このことは１枚のＣＤ－ＲＯＭディスク１について、各セクタ毎に暗号キーを変更してしまう本実施例の構成についても当然該当するものであり、低コストで第三者の解読が極めて難しい暗号記録が可能である。

【００４３】次に図４乃至図６を参照して、コンピュータシステムにおいて所定の記録制御プログラム及び再生制御プログラムを実行させることにより、ＣＤ－ＲＯＭディスク１の記録、再生を前述の実施例の場合と同様にして行うようにした他の実施例について説明する。

【００４４】図４は、ＣＤ－ＲＯＭディスク１に、外部記憶装置３１内に格納されているユーザデータを暗号化して記録すると共に、暗号化して記録されているユーザデータをＣＤ－ＲＯＭディスク１から読み出して再生するための、コンピュータシステムを利用した本発明によるＣＤ－ＲＯＭ記録・再生システム３０の概略構成図である。

【００４５】図４で、ＣＤ－ＲＯＭマスタリング装置１８及びＣＤ－ＲＯＭドライブ装置２１は図１及び図２に示されている各装置と同一のものであり、これらの装置１８、２１及び外部記録装置３１はコンピュータシステム３２に接続されている。符号３８で示されるのはキーボードである。

【００４６】このコンピュータシステム３２は、中央演算処理装置（ＣＰＵ）３３、ランダムアクセスメモリ（ＲＡＭ）３４、読出し専用メモリ（ＲＯＭ）３５及び入出力インターフェイス装置（Ｉ／Ｆ）３６がバス３７によって相互に接続されて成る公知の構成である。そして、ＲＯＭ３５内に格納されている記録制御プログラム及び再生制御プログラムがＣＰＵ３３において実行されることにより、図１及び図２に示した構成の場合と同様にして、ＣＤ－ＲＯＭディスク１への暗号化ユーザデータの記録、及びこのようにして記録された暗号化ユーザデータの再生、復号化が実行される。

【００４７】先ず、図５を参照しながら、ＣＤ－ＲＯＭ記録・再生システム３０による記録動作について説明する。

【００４８】記録制御プログラムの実行が開始されると、先ずステップ４１でキーボード３８から入力される暗号化対象セクタを示すデータに従って暗号化対象セクタが決定される。次のステップ４２では、暗号化が必要な各セクタの暗号キーが生成され、生成された暗号キーが暗号キーデータとしてＲＡＭ３４内に格納される。この暗号キーデータは図１に基づいて説明したものと同様である。

【００４９】ステップ４３では、ＣＤ－ＲＯＭマスタリング装置１８が暗号キー記録セクタ３への書き込み状態になっているか否かが判別される。ＣＤ－ＲＯＭマスタリング装置１８が暗号キー記録セクタ３への書き込み状態になっていると、ステップ４３の判別結果はＹＥＳと

なり、ステップ４４に進む。ステップ４４では、ＲＡＭ３４に格納されている暗号キーデータがＣＰＵ３３及びＩ／Ｆ３６を経由してＣＤ－ＲＯＭマスタリング装置１８に送られ、ＣＤ－ＲＯＭマスタリング装置１８にセットされているＣＤ－ＲＯＭディスク１の暗号キー記録セクタ３に暗号キーデータが記録される。しかる後、ステップ４９で所要のユーザデータが全て記録されたか否かの終了チェックが行われ、全ての記録がまだ終了していない場合にはステップ４３に戻る。

【００５０】暗号キーデータの記録が終了した時点ではステップ４３の判別結果はＮＯとなり、ステップ４５において１セクタ分のユーザデータが外部記憶装置３１から読み込まれる。次のステップ４６では、この読み込まれた１セクタ分のユーザデータを記録すべきセクタが暗号化対象セクタになっているか否かが判別される。その１セクタ分のユーザデータを記録すべきセクタが暗号化対象セクタであると、ステップ４６の判別結果はＹＥＳとなり、ステップ４７に入る。

【００５１】ステップ４７では、ステップ４２で生成された暗号キーのうちそのセクタのための暗号キーを用いて１セクタ分のユーザデータを暗号化するための処理を行い、次のステップ４８で暗号化処理された１セクタ分のユーザデータをＣＤ－ＲＯＭマスタリング装置１８に送る。ＣＤ－ＲＯＭマスタリング装置１８は受け取った１セクタ分のユーザデータを所要のセクタに記録する。

【００５２】ステップ４６の判別結果がＮＯの場合にはステップ４７は実行されないので、外部記憶装置３１から読み込まれた１セクタ分のユーザデータは暗号化処理されず、そのままＣＤ－ＲＯＭマスタリング装置１８に送られ、所要のセクタに記録される。

【００５３】このようにして、ユーザデータが全てＣＤ－ＲＯＭディスク１に書き込まれると、ステップ４９の判別結果がＹＥＳとなり、記録制御プログラムの実行が終了する。

【００５４】次に、このようにしてＣＤ－ＲＯＭディスク１に記録されたデータをＣＤ－ＲＯＭディスク１から読み出し再生するためのＣＤ－ＲＯＭ記録・再生システム３０の再生、復号化動作について、図６を参照しながら説明する。

【００５５】再生制御プログラムの実行開始後、先ずステップ５１においてＣＤ－ＲＯＭディスク１の入替ありか否かが判別される。入替ありの場合にはステップ５２に進み、ここで、暗号キー記録セクタ３に記録されている暗号キーデータが読み込まれステップ５３に進む。ステップ５１の判別結果がＮＯの場合には、既に暗号キーデータの読み込みはなされているので、ステップ５２は実行されず、ステップ５３に入る。

【００５６】ステップ５３では、ＣＤ－ＲＯＭドライブ装置２１によってＣＤ－ＲＯＭディスク１から１セクタ分のデータを読み込み、ステップ５４でこの読み込まれた１セクタ分のデータが復号化対象セクタのデータであるか否かが判別される。それが復号化対象セクタであるとステップ５５に入り、ステップ５２で既に読み込まれている暗号キーデータのうちのそのセクタに対応する暗号キーデータを用いて所要の復号化処理が行われ、ステップ５６に進む。一方、ステップ５３で読み込まれた１セクタ分のデータが復号化対象セクタのデータでない場合には、ステップ５５を実行することなしにステップ５６に入る。

【００５７】ステップ５６では、全ての必要セクタの読み込みが終了したか否かが判別され、全ての必要セクタの読み込みが未だ終了していない場合にはステップ５３に戻る。このようにして、ＣＤ－ＲＯＭディスク１に記録されたデータが１セクタ毎に読み込まれ、復号化の必要なセクタについてのみ復号化処理が実行される。全ての必要セクタの読み込みが終了すると、ステップ５６での判別結果がＹＥＳとなり、再生制御プログラムの実行が終了する。このようにして、ＣＤ－ＲＯＭディスク１に記録されたユーザデータを再生、復号化することができる。

【００５８】図４に示したＣＤ－ＲＯＭ記録・再生システム３０もまた、図１及び図２に示したシステムの場合と同様の利点を有している。

【００５９】

【発明の効果】本発明による効果は以下の通りである。

【００６０】ＣＤ－ＲＯＭディスクに記録すべきデータを暗号化するのに使用された暗号キー情報が暗号化されたデータを記録するＣＤ－ＲＯＭディスク内に記録されるので、暗号キー情報を別途管理する必要がない。したがって、暗号キー情報の管理のためのコストが不要であるばかりか、その管理の煩わしさから解放される。

【００６１】暗号化データと暗号キー情報とを同一のＣＤ－ＲＯＭディスク中に記録するので、暗号キーをどのように変更したとしてもこの変更に関する情報を別途に記録、管理しておく必要はなく、ＣＤ－ＲＯＭディスク内のデータの再生時には復号化に必要な暗号キーをそのＣＤ－ＲＯＭディスクから読み出すだけでよいから、復号化に要する手間が著しく簡素化される。

【００６２】本発明の方式によりデータの暗号化記録が行われることによって、暗号化データとこれを解読するための暗号キー情報とが一緒に記録されているＣＤ－ＲＯＭディスクは、ＣＤ－ＲＯＭディスクに対応する暗号キー情報の管理という概念はなく、暗号キー情報管理は全て不要になり、その管理コストを不要にすることができるほか、暗号化を全く意識することなしにユーザデータの再生、復号化を行うことができる。

【００６３】暗号キー情報の管理コストが全く問題とならないので、例えばＣＤ－ＲＯＭディスク毎に異なった暗号キーを使用しても何らの管理コストを発生させることがなく、記録の機密保持をコストを生じさせることな

11

しに著しく向上させることができる。

【図面の簡単な説明】

【図１】本発明によるＣＤ－ＲＯＭディスクの記録システムの一実施例を示す構成図。

【図２】本発明によるＣＤ－ＲＯＭディスク再生システムの一実施例を示す構成図。

【図３】図１及び図２のシステムにおいて使用されるＣＤ－ＲＯＭディスクの記録方式を説明するためのＣＤ－ＲＯＭディスク内の記録領域の説明図。

【図４】本発明によるＣＤ－ＲＯＭディスク記録・再生システムの他の実施例を示す構成図。

【図５】図４のコンピュータシステムにおいて実行される記録制御プログラムを示すフローチャート。

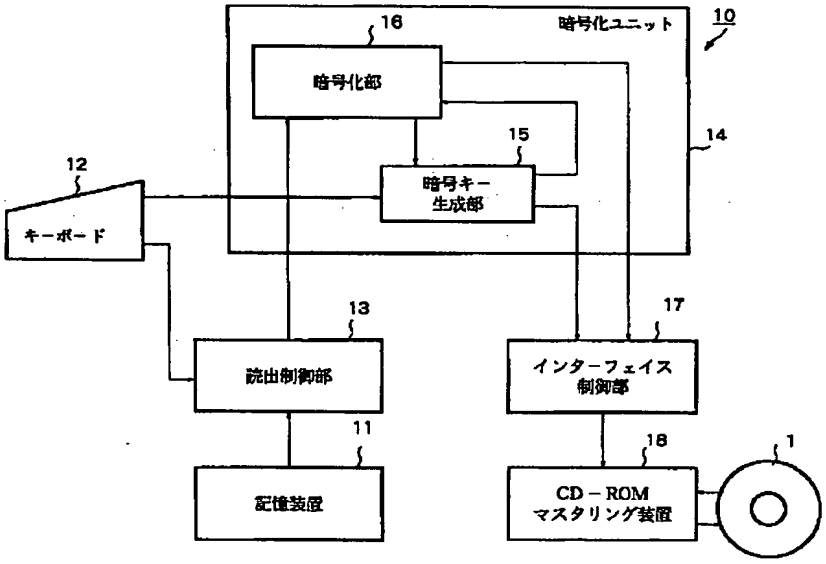
【図６】図４のコンピュータシステムにおいて実行される再生制御プログラムを示すフローチャート。

12

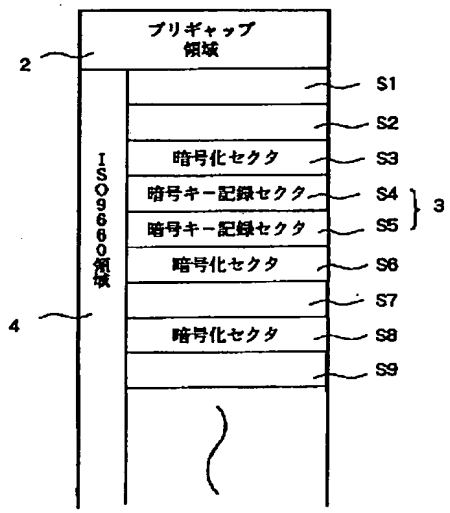
【符号の説明】

１　ＣＤ－ＲＯＭディスク
３　暗号キー記録セクタ
４　ＩＳＯ９６６０領域
１０　ＣＤ－ＲＯＭ記録システム
１１　記憶装置
１４　暗号化ユニット
１５　暗号キー生成部
１６　暗号化部
２０　ＣＤ－ＲＯＭ再生システム
２３　復号化ユニット
２４　復号化部
３０　ＣＤ－ＲＯＭ記録・再生システム
Ｓ１乃至Ｓ９　セクタ

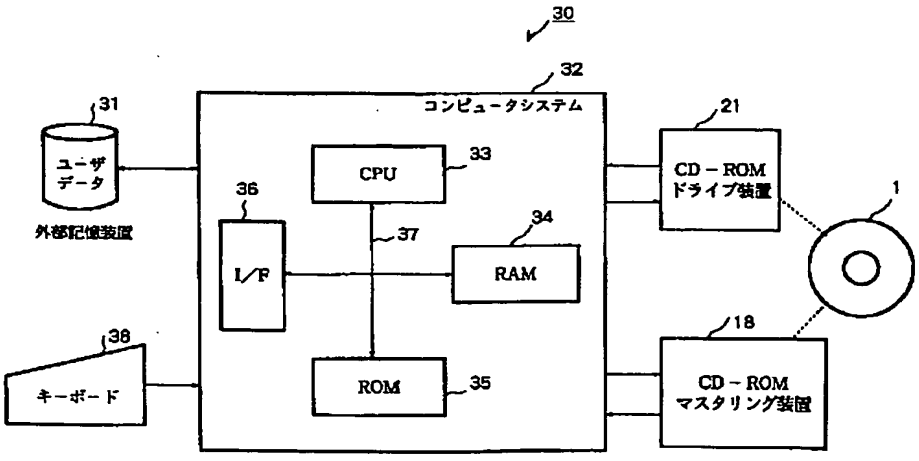
【図１】



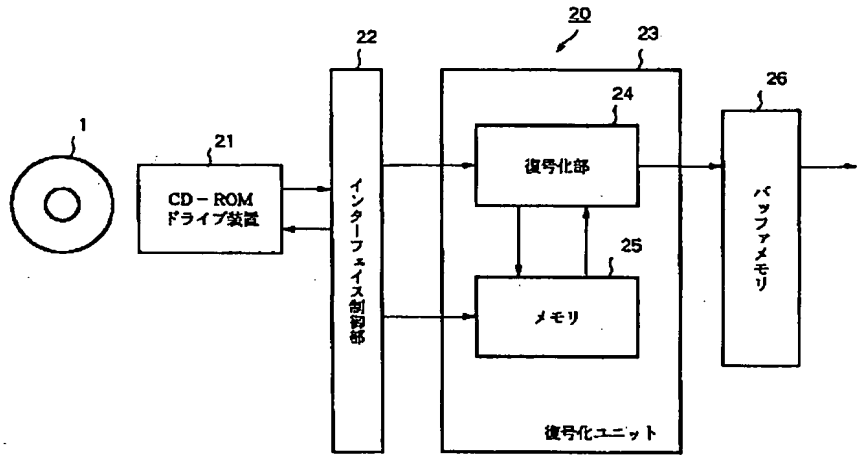
【図３】



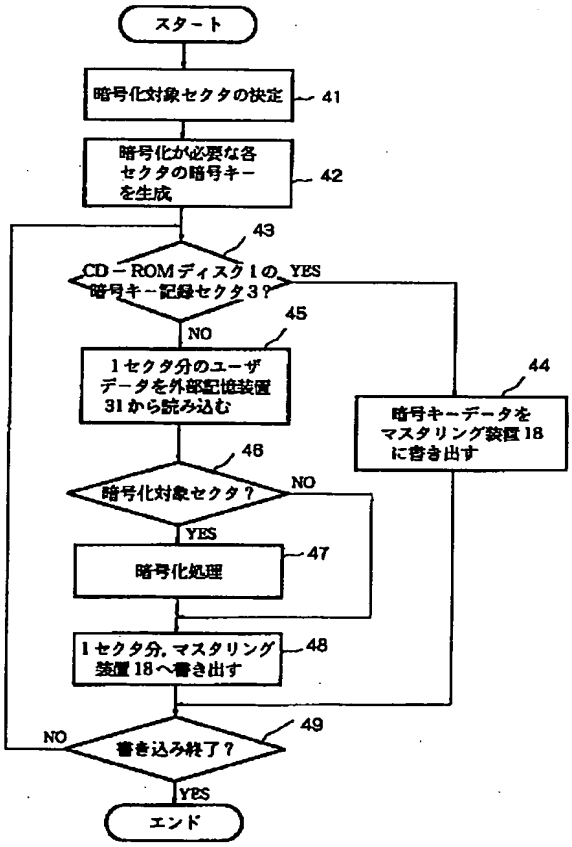
【図４】



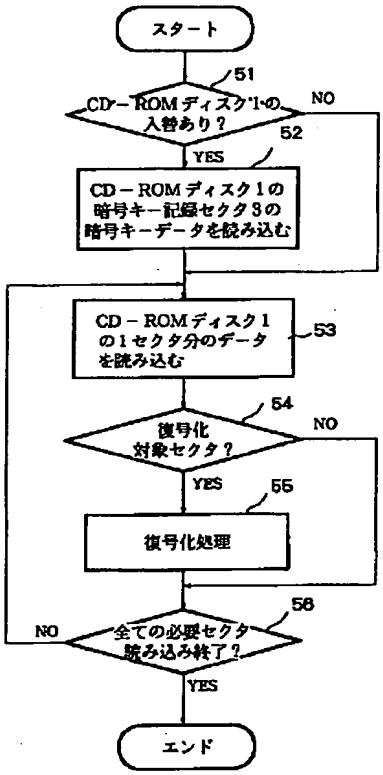
【図２】


1
21
CD－ROM
ドライブ装置
22
インターフェイス制御部
20
23
24
復号化部
25
メモリ
26
バッファメモリ
復号化ユニット

【図５】


スタート
暗号化対象セクタの決定
41
暗号化が必要な各セクタの暗号キーを生成
42
43
CD－ROMディスク1の暗号キー記録セクタ3？
YES
NO
45
1セクタ分のユーザデータを外部記憶装置31から読み込む
44
暗号キーデータをマスタリング装置18に書き出す
46
暗号化対象セクタ？
NO
YES
暗号化処理
47
1セクタ分，マスタリング装置18へ書き出す
48
49
書き込み終了？
NO
YES
エンド

【図６】


スタート
51
CD－ROMディスク1の入替あり？
NO
52
YES
CD－ROMディスク1の暗号キー記録セクタ3の暗号キーデータを読み込む
CD－ROMディスク1の1セクタ分のデータを読み込む
53
54
復号化対象セクタ？
NO
YES
55
復号化処理
56
NO
全ての必要セクタ読み込み終了？
YES
エンド

フロントページの続き

(72)発明者　谷口　利典
愛知県名古屋市瑞穂区苗代町15番１号　ブラザー工業株式会社内